

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-071037
(43)Date of publication of application : 05.03.1992

(51)Int.Cl. G06F 11/16
G06F 11/14
G06F 11/18
G06F 15/16

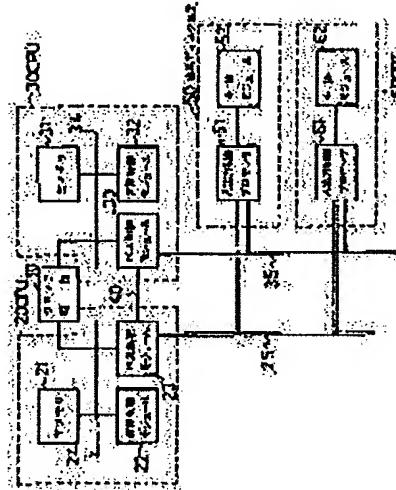
(21)Application number : 02-184614 (71)Applicant : TOSHIBA CORP
(22)Date of filing : 12.07.1990 (72)Inventor : TAKAHASHI CHIKAYOSHI

(54) DUPLEX SYSTEM FOR ELECTRONIC COMPUTER

(57)Abstract:

PURPOSE: To secure the high reliability of output data to a peripheral device without duplexing an internal circuit and an internal bus by executing plural abnormality generation specifying means in stages and specifying a CPU generating abnormality.

CONSTITUTION: When 'inconsistent error' information is continuously outputted from respective bus control modules 23, 33 to arithmetic control modules (ACPs) 22, 32 even when retrying processing is executed, a task being executed at present is abnormally ended as the 2nd specifying means and then retrying processing at a task level is executed. If the 'inconsistent error' is continued even when the retrying processing at the task level is executed, the operation check of hardware is executed by a test program controlled by an operation systems as the 3rd error specifying means, a fault generating position on the hardware is diagnosed and the CPU generating the abnormality can be specified.



X

⑩日本国特許庁 (JP) ⑪特許出願公開

⑫公開特許公報 (A) 平4-71037

⑬Int. Cl. 5

G 06 F 11/16
11/14
11/18
15/16

識別記号

310 C
310 C
470 J

府内整理番号

9072-5B
9072-5B
9072-5B
9190-5L

⑭公開 平成4年(1992)3月5日

審査請求 未請求 請求項の数 1 (全8頁)

⑮発明の名称 電子計算機の二重化方式

⑯特 願 平2-184614

⑰出 願 平2(1990)7月12日

⑱発明者 高橋 力 良 東京都府中市東芝町1番地 株式会社東芝府中工場内

⑲出願人 株式会社東芝 神奈川県川崎市幸区堀川町72番地

⑳代理人 弁理士 鈴江 武彦 外3名

明細書

1. 発明の名称

電子計算機の二重化方式

2. 特許請求の範囲

2台のCPUを用いてフォールトトレラント・コンピュータシステムを構成する電子計算機の二重化方式において、

上記2台のCPUそれぞれのバス制御モジュールに備えられた自CPUと相手方CPUの出力データ同士の一致/不一致を比較検出する出力比較手段と、

この出力比較手段によりデータ不一致が検出された場合にバス制御モジュールからのデータ出力動作を停止させるデータ出力停止手段と、

上記出力比較手段によりデータ不一致が検出された場合にその不一致情報をCPUに対して通知する比較情報通知手段と、

この比較情報通知手段によりCPUに不一致情報が通知された際に所定回数のリトライ処理を実施する第1の異常特定化手段と、

この第1の異常特定化手段を行なった際に上記比較情報通知手段によりCPUに継続して不一致情報が通知されている場合にはオペレーションシステムにより管理されるテストプログラムを実行する第2の異常特定化手段と、

この第2の異常特定化手段を行なった際に上記比較情報通知手段によりCPUに継続して不一致情報が通知されている場合には上記コンピュータシステムの停止/再起動処理を実施するシステム復帰手段とを具備したことを特徴とする電子計算機の二重化方式。

3. 発明の詳細な説明

【発明の目的】

(産業上の利用分野)

本発明は、フォールトトレラント・コンピュータシステムを構成する際に、CPUを中心とする構成要素を二重化することによりシステムの信頼性及び可用性を向上させる電子計算機の二重化方式に関する。

(従来の技術)

一般に、フォールトトレラント・コンピュータシステムを完全なハードウェア構成により実現するには、CPUを中心とする構成機器の内部を二重化することが行なわれる。

このシステム二重化の一例としては、システムを構成する各モジュールをそれぞれ2台用いると共に、この二重化された各モジュール間を結合するバスラインを二重化したもののが実用されているが、最近では、CPUを始め、各主要モジュールの内部回路までも二重化して、その二重化回路間の処理結果を比較することが行なわれている。

第3図は従来の二重化方式によるフォールトトレラント・コンピュータシステムの構成を示すもので、CPU11を始めメモリ12、磁気ディスク制御装置13及び磁気ディスク装置14、通信制御装置15からなる1組のコンピュータシステムがそのまま二重化され、そのそれぞれが二重化されたバスラインにより結合されている。そして、各CPU11、11の内部には、さらに2つの

データが一致することを確認した後に両方のバスに対して出力される。

また、CPU11が磁気ディスク装置14に対してデータの書き込みを行なうときは、CPU11はバスに出力を行なう最終段で各ACP16a、16bからのデータ比較を行ないそのエラーチェックを実施する。この場合、CPU11においてデータエラーが検出されなければ、磁気ディスク制御装置13の入力段に伝送されたデータには、バス上におけるノイズ等の要因以外にエラーが発生することは殆どない。したがって、CPU11から2本のバスを介して伝送されたデータを、磁気ディスク制御装置13の入力段における比較はせずに、該磁気ディスク制御装置13から次段のモジュール、つまり、磁気ディスク装置14への出力段で上記二重化データの比較が行なわれる。この場合、1度の比較処理で、バスから磁気ディスク制御装置13へのデータ入力に伴うエラー、及び磁気ディスク装置13内でのデータ処理に伴うエラーを検出することができる。

ACP(演算制御モジュール)16a、16bが設けられると共に、メモリ12、磁気ディスク制御装置13、通信制御装置15の各内部回路も二重化されている。この場合、上記バスラインの二重化に伴い、各モジュールにおけるバスへの出力は2系統、また、バスから各モジュールへの入力も2系統あることになる。

このフォールトトレラント・コンピュータシステムにおいて、通常、各モジュールにおける処理結果の比較は、そのそれぞれのモジュールの最終出力段において実施されるので、当該モジュールで発生するエラーは確実に検出することができる。

すなわち、例えばCPU11と磁気ディスク制御装置13との間のデータ転送を想定した場合に、CPU11が磁気ディスク装置14からデータの読み出しを行なうときは、磁気ディスク制御装置13はバスに対して出力の動作モードにある。このとき、磁気ディスク制御装置13における処理結果はバスへの出力直前に比較され、2系統の

ここで、バスライン上でエラー発生要因について説明する。

例えば、出力モードにあるモジュールは、バスに出力するデータに関してエラーチェックを実施している。したがって、本来なら、バス上に預けたデータが出力されることはない。しかし、この出力モードにあるモジュールのバスに直接接続されているゲートの故障や、バス上の信号のクロストークノイズ等に起因するエラーの場合には、該出力モジュールにおけるエラー検出に掛からず、入力モジュール側の処理結果比較段階で検出されることになる。

このような、バス上でのデータエラーは、二重化したモジュールの両方でエラーを発生させてしまう致命傷である。

すなわち、2本あるバスの両方でデータエラーが発生した場合には、各システムモジュールが2台あろうと、各モジュール内部が完全に二重化してあろうとも、何れのモジュールに入力されるデータにも誤りが生じ、その処理結果が異常になっ

てこのコンピュータシステムはエラーになる。

また、2本あるバスのうち一方のバスのみでデータエラーが発生した場合には、入力モジュールにおいて、その内部で二重化してある回路のうち一方の回路が誤ったデータを用いて処理を行なうため、該二重化内部回路の処理結果に相違が生じる。したがって、両方の入力モジュールともその出力段での比較結果は異常になり、このコンピュータシステムはエラーになる。

近年、電子計算機における処理性能の向上は著しく、システム動作の基本グローブはより高周波になり、使用する素子も信号の立上り／立下りが急速なものになっている。しかも、コンピュータシステムの大規模化は、バスに接続されるモジュール数の増加をもたらすばかりでなく、バスそのものの延長をもたらし、バス上において信号の信頼性を損い易い傾向にある。すなわち、バス上において、クロストークや信号の反射等による断続的なエラーを発生し易く、しかも、CPUが高速化するのに伴い、多数のモジュールをバスを介

して接続するのは困難になっている。

（発明が解決しようとする課題）

しかしながら、上記のような従来の二重化方式によるフォールトトレラント・コンピュータシステムでは、CPUを中心とするコンピュータシステムを2組並列にして二重化を図るばかりでなく、個々のモジュールの内部回路をも二重化し、外部バス及び内部バス共に二重化した完全二重化を図っているので、ハードウェアの構成が大掛かりになりシステム構築のコスト上昇を招くばかりでなく、バス上でのエラー発生も招き易くなり、しかも、個々のCPU内部で二重化されたACP同士で直接処理データの比較を行なうため、高速化達成の妨げになる。

本発明は上記課題に鑑みなされたもので、高速CPUを用いたフォールトトレラント・コンピュータシステムを構築する際に、2つのCPUそれぞれにおける内部回路の二重化及び内部バスの二重化を行うことなく、周辺装置に対する出力データの高信頼性を確保することが可能になる電子計

算機の二重化方式を提供することを目的とする。

【発明の構成】

（課題を解決するための手段）

すなわち、本発明に係わる電子計算機の二重化方式は、2台のCPUを用いてフォールトトレラント・コンピュータシステムを構成するもので、上記2台のCPUそれぞれのバス制御モジュールに備えられたCPUと相手方CPUの出力データ同士の一一致／不一致を比較検出する出力比較手段と、この出力比較手段によりデータ不一致が検出された場合にバス制御モジュールからのデータ出力動作を停止させるデータ出力停止手段と、上記出力比較手段によりデータ不一致が検出された場合にその不一致情報をCPUに対して通知する比較情報通知手段と、この比較情報通知手段によりCPUに不一致情報が通知された際に所定回数のリトライ処理を実施する第1の異常特定化手段と、この第1の異常特定化手段を行なった際に上記比較情報通知手段によりCPUに継続して不一致情報が通知されている場合にはオペレーションシス

テムにより管理されるテストプログラムを実行する第2の異常特定化手段と、この第2の異常特定化手段を行なった際に上記比較情報通知手段によりCPUに継続して不一致情報が通知されている場合には上記コンピュータシステムの停止／再起動処理を実施するシステム復帰手段とを備えてなるものである。

（作用）

つまり、バス制御モジュールからCPUの中核となる演算制御モジュールに対して出力データの不一致情報が通知された際に、データ出力動作を停止させると共に、複数の異常発生特定化手段を段階的に実施して異常発生CPUの特定化を行ない、この段階的な異常発生特定化手段により異常発生CPUが特定されない場合には、さらに、システム停止／再起動処理を実施することで異常データが解消されるようになる。

（実施例）

以下図面により本発明の一実施例について説明する。

第1図は本発明の電子計算機の二重化方式に基づくフォールトトレラント・コンピュータシステムの構成を示すもので、同図において、20, 30は二重化されたCPUであり、各CPU20, 30にはそれぞれ主メモリ(MEM)21, 31、演算制御モジュール(ACP)22, 32、バス制御モジュール23, 33が備えられ、それぞれ内部バス24, 34を介して信号の授受が行なわれる。

バス制御モジュール23, 33は、CPU内部バス24, 34と外部バス25, 35との間の信号の授受を制御すると共に、CPU間同期ケーブル40を介して相手方バス制御モジュールとの出力信号の比較を行なうもので、外部バス25, 35には、磁気ディスク装置50及びCRT60が周辺装置として接続される。また、各CPU20, 30の内部バス24, 34間には、該CPU20, 30を同期制御するためのクロック回路10が接続される。

一方、磁気ディスク装置50及びCRT60に

出力比較回路232, 332は、それぞれ自方のCPUが外部バスに出力する信号と、他方のCPUが外部バスに出力する信号とを、前記CPU間同期ケーブル40を介して比較しその一致/不一致を検出するもので、この出力比較回路232, 332からの一致/不一致信号は、各対応する比較結果通知ライン233, 333を介して主論理回路231, 331に出力される。

次に、上記構成によるフォールトトレラント・コンピュータシステムの動作について説明する。

まず、CPU20, 30が磁気ディスク装置50にデータ転送を行なう場合に、演算制御モジュール(ACP)22, 32から磁気ディスク装置50への入出力動作起動命令や、その後に主メモリ(MEM)21, 31から送られる各種のデータは、高速な内部バス24, 34を介してバス制御モジュール23, 33に送られ、外部バス25, 35用の信号伝送タイミング及びデータ伝送幅に変換されて該外部バス25, 35に出力される。すると、この外部バス25, 35に出力さ

は、上記2本の外部バス25, 35に接続するための2ポートの入出力端子を有する入出力制御プロセッサ51及び61が備えられ、磁気ディスク装置50の入出力制御プロセッサ51には磁気ディスク本体モジュール52が接続され、また、CRT60の入出力制御プロセッサ61にはCRT本体モジュール62が接続される。

第2図は上記2つのCPU20, 30のバス制御モジュール23, 33の内部構成を示すもので、内部バス24, 34及び外部バス25, 35は、各バス制御モジュール23, 33の主論理回路231, 331に接続される。この主論理回路231, 331は、内部バス24, 34から与えられた信号のパリティチェックを行なうと共に、内部バス24, 34と外部バス25, 35との間で伝送信号のタイミング変換やデータ幅変換等の処理を実行するもので、この主論理回路231, 331には、出力比較回路232, 332からの比較結果信号が比較結果通知ライン233, 333を介して供給される。

されたデータは磁気ディスク装置50の入出力制御プロセッサ51に取込まれ磁気ディスク本体モジュール52に送られる。そして、磁気ディスク本体モジュール52において転送データの書き込みが実行される。

ここで、両方のCPU20, 30からの出力データが正常である場合には、外部バス25と35とはそれぞれ同じ内容のデータを流しているので、各バス制御モジュール23, 33における出力比較回路232, 332からは、それぞれ対応する比較結果通知ライン233, 333を介して主論理回路231, 331に出力一致を示す信号が送られる。この場合、それ以後の動作が継続される。

また、例えば一方のCPU30からの出力データに誤りがある場合に、出力比較回路332で検出されるデータ誤りの形態は2通りに大別される。つまり、第1のエラー形態は、主メモリ(MEM)31及びバス制御モジュール33が付与したパリティ情報によりエラーとして認識できるもので、これは上記主メモリ(MEM)31あるいはバス

制御モジュール33の故障や内部バス34上の障害に起因する。また、第2のエラー形態は、上記バリティエラーに掛からないもので、この原因としては、内部バス34上で発生した2ビット以上の誤りや何等かの原因で主メモリ(MEM)31に書き込まれていた誤データの読み出し等がある。

すなわち、上記第1のエラー形態として、内部バス34上のデータにバリティエラーが発生した場合には、バス制御モジュール33における主論理回路331の内部にありバスを監視しているバリティ検出回路においてエラーが検出され、外部バス35への出力が禁止されると共に、演算制御モジュール(ACP)32に対してエラーが通知される。すると、上記CPU30の演算制御モジュール(ACP)32は、故障箇所修復の後、相手方CPU20との間で同期運転に復帰するための制御を実行し、2台のCPU20, 30による通常動作に戻る。

また、上記第2のエラー形態として、CPU30の主メモリ(MEM)31に記憶されている

これにより、各CPU20, 30におけるバス制御モジュール23, 33の入出力動作が中断されると共に、それぞれ外部バス25, 35を介し各周辺装置50, 60の入出力制御プロセッサ51, 61にエラー発生が通知され、また、これと同時に、各CPU20, 30の演算制御モジュール(ACP)23, 33に対して「不一致エラー発生」が通知される。

このとき、各CPU20, 30においては、データエラーの原因がどちら側にあるかを特定できないため、上記「不一致エラー」が発生した場合には、先ず、第1のエラー特定化手段として、所定回数のデータ再送処理(リトライ)が実施される。

すなわち、上記主メモリ(MEM)31の内容が誤った原因が一過性のものであった場合、上記リトライ処理の過程で該誤データが正常なデータに復帰することが考えられる。この場合、例えば内部バス34上で発生したノイズ等に起因する一過性のエラーに対しても同様の作用が得られる。

データに誤りが生じている場合には、演算制御モジュール(ACP)32は自方CPU30内のメモリ情報に異常があることを認識していないので(認識していれば、自CPU異常としてシステム再構成の処理を実行し、異常箇所の修復後通常運転に復帰する)、該誤データが内部バス34を経てバス制御モジュール33に出力される際には正しくバリティ情報が付与される。このため、バス制御モジュール33の主論理回路331が上記誤データを受信した時点ではバリティエラーは検出されないが、外部バス35に出力するデータとCPU間同期ケーブル40を介して取込んだ相手方外部バス25からの出力データとは一致しなくなるので、バス制御モジュール33における出力比較回路332からは比較結果通知ライン333を介して「不一致」を示す信号が主論理回路331に送られると共に、相手方CPU20における出力比較回路232でもデータ不一致エラーが検出され、「不一致」を示す信号が主論理回路231に送られる。

また、上記主メモリ(MEM)31において、メモリ情報が誤ったまま固定されていた場合でも、上記リトライ処理を実施している過程で、プログラム上に矛盾が発生したり、あるいはウォッチドッグタイマー(時間監視プログラム)でエラー検出されることにより、一方のCPU30によるプログラム処理が停止されるようになり、異常発生CPUの特定化が行なわれる。これにより、システム再構成と修復の処置に入ることができる。

次に、上記所定回数のリトライ処理を実施しても、それぞれのバス制御モジュール23, 33から演算制御モジュール(ACP)23, 32に対し「不一致エラー」の通知が続く場合には、第2のエラー特定化手段として、現在実行中のタスクがアブノーマルエンドされ、代ってタスクレベルでのリトライ処理が実施される。

この場合、上記第1のエラー特定化手段によるリトライ処理よりも、広範囲なプログラムでのリトライが実施されることになり、上記同様の作用により異常発生CPUの特定化が行なわれる。

さらに、上記タスクレベルでのリトライ処理を実施しても、それぞれのバス制御モジュール 23, 33 から演算制御モジュール (ACP) 22, 32 に対し「不一致エラー」の通知が続く場合には、第 3 のエラー特定化手段として、オペレーションシステム (OS) で管理されるテストプログラムによりハードウェアの動作チェックが実施される。これにより、ハードウェア上のフォールト発生箇所が診断され、異常発生 CPU の特定化が行なわれる。

そして、上記テストプログラムを動作させても何等異常が検出されない場合には、システム復帰手段として、現在実行中のシステム動作が一旦停止され再起動が実施される。これにより、主メモリ (MEM) 31 上の誤データは解消されることになり、正常運転に復帰できるようになる。つまり、この場合、磁気ディスク本体モジュール 52 においてデータの完全な保存が図られているので、システム再起動時には、主メモリ (MEM) 31 上の誤データは正しいデータに書き換えること

になる。

したがって、上記構成のフォールトトレラント・コンピュータシステムによれば、二重化した CPU 20, 30 の各バス制御モジュール 23, 33 において、自 CPU からの出力データと相手方 CPU からの出力データとの一致／不一致を比較検出し、該バス制御モジュール 23 または 33 から演算制御モジュール 22 または 32 に対して出力データの不一致エラーが通知された際には、データ出力動作を停止させると共に、①データ再送処理、②タスクレベルでのリトライ処理、③テストプログラムによるハードウェアの動作チェックを段階的に実施して異常発生 CPU の特定化を行ない、この段階的なエラー特定化手段により異常発生 CPU が特定されない場合には、さらに、システム停止／再起動処理を実施してエラーデータの解消を行なうので、確実に異常発生 CPU を特定しあるいは異常発生箇所を解消して、周辺装置に対する出力データの高信頼性を確保することができる。

適用することができる。

【発明の効果】

以上のように本発明によれば、2 台の CPU を用いてフォールトトレラント・コンピュータシステムを構成するもので、上記 2 台の CPU それぞれのバス制御モジュールに備えられ自 CPU と相手方 CPU の出力データ同士の一致／不一致を比較検出する出力比較手段と、この出力比較手段によりデータ不一致が検出された場合にバス制御モジュールからのデータ出力動作を停止させるデータ出力停止手段と、上記出力比較手段によりデータ不一致が検出された場合にその不一致情報を CPU に対して通知する比較情報通知手段と、この比較情報通知手段により CPU に不一致情報が通知された際に所定回数のリトライ処理を実施する第 1 の異常特定化手段と、この第 1 の異常特定化手段を行なった際に上記比較情報通知手段により CPU に粗続して不一致情報が通知されている場合にはオペレーションシステムにより管理されるテストプログラムを実行する第 2 の異常特定化

この場合、各 CPU 20, 30 それぞれの内部回路までも二重化する事がないので、従来の二重化方式に比較して少ないハードウェアでフォールトトレラント・コンピュータシステムを実現でき、システム構築コストの上昇を防止できると共に、内部バス上でのエラー発生を抑制することができる。また、上記二重化 CPU 20, 30 同士の出力データ比較処理を、該 CPU 20, 30 の中枢である演算制御モジュール (ACP) 22, 32 では行なわずに、バス制御モジュール 23, 33 において行なうので、CPU 自体の処理速度の高速化が妨げられることなく、比較的低速な出力比較回路 232, 332 を用いて安定したエラー検出動作を得ることができ、しかも、上記 CPU の内部、つまり、演算制御モジュール (ACP)、主メモリ (MEM)、内部バスを通過した一貫したエラーチェックを行なうことができる。

尚、上記実施例における電子計算機の二重化方式は、マイクロプロセッサ応用製品の全般に対し

手段と、この第2の異常特定化手段を行なった際には上記比較情報通知手段によりCPUに継続して不一致情報が通知されている場合には上記コンピュータシステムの停止／再起動処理を実施するシステム復帰手段とを備え、確実に異常発生CPUを特定するかあるいは異常発生箇所を解消できるので、高速CPUを用いたフォールトトレラント・コンピュータシステムを構築する際に、2つのCPUそれぞれにおける内部回路の二重化及び内部バスの二重化を行なうことなく、周辺装置に対する出力データの高信頼性を確保することが可能になる。

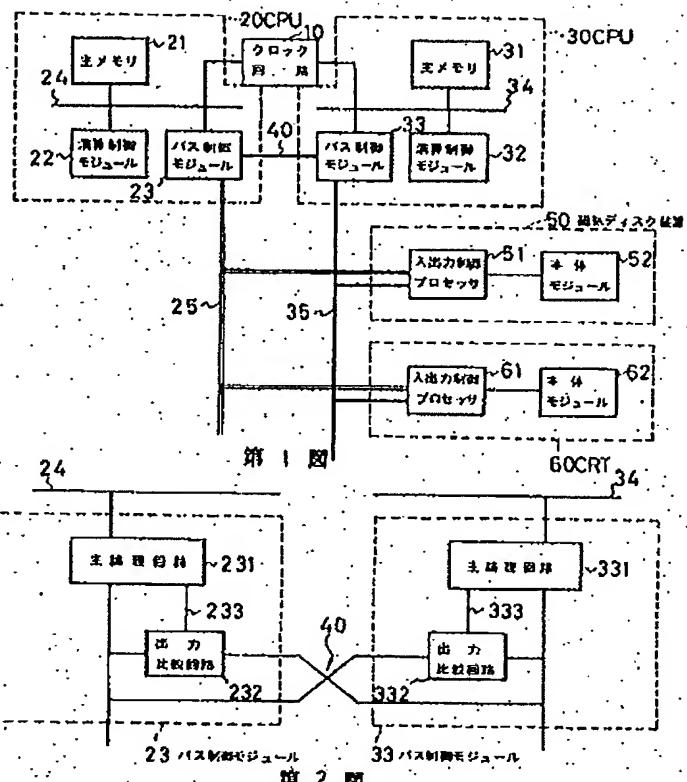
4. 図面の簡単な説明

第1図は本発明の電子計算機の二重化方式の一実施例に係わるフォールトトレラント・コンピュータシステムの構成を示すブロック図、第2図は上記フォールトトレラント・コンピュータシステムにおける2つのCPUのバス制御モジュールの内部構成を示すブロック図、第3図は従来の二重化方式によるフォールトトレラント・コンピュータ

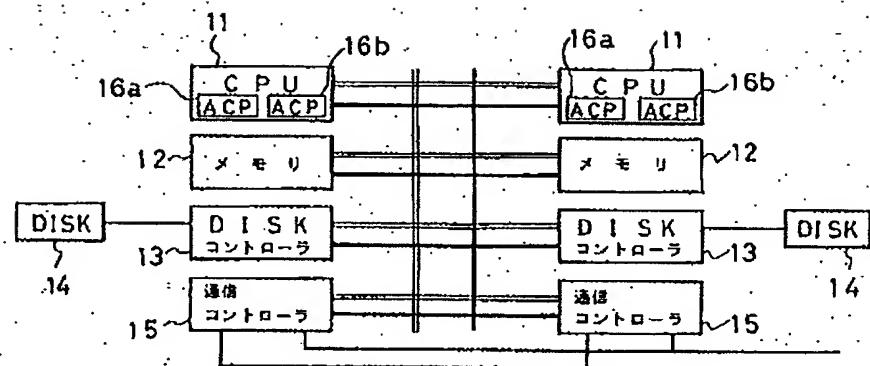
システムの構成を示すブロック図である。

10…クロック回路、20, 30…CPU、
21, 31…主メモリ(MEM)、22, 32…
演算制御モジュール(ACP)、23, 33…バ
ス制御モジュール、24, 34…内部バス、25,
35…外部バス、40…CPU間同期ケーブル、
50…磁気ディスク装置、51, 61…入出力制
御プロセッサ、52…磁気ディスク本体モジュー
ル、62…CRT本体モジュール、231,
331…主論理回路、232, 332…出力比較
回路、233, 333…比較結果通知ライン。

出願人代理人、弁理士 鈴江武彦



第2図



第3圖